Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 27, 2009

Name of Company covered by this certification: D&E Networks, Inc.

Form 499 Filer ID: 804682

Name of signatory: Albert H. Kramer

Title of signatory: Vice President, Assistant Secretary/Treasurer

I, Albert H. Kramer, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed Albert H. Kramer 2/18/09

Statement of CPNI Operating Procedures and Policies

D&E Networks, Inc. (the "Company") has operating procedures designed to ensure that the Company is in compliance with the FCC's Customer Proprietary Network Information ("CPNI") rules.

The Company has implemented a system by which the status of a customer's CPNI approval can be clearly established by Company personnel prior to their use of CPNI. Specifically, the main screen on a customer's account has a flag indicating the customer's approval, or denial, for the Company to use, disclose, or access the customer's CPNI. In addition, prior to marketing any service, the Company generates a list of customers based on the CPNI approval status of each account.

The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to customer CPNI. The Company will release CPNI to customers through in-store contact with a valid photo ID. The Company has implemented a password system for the release of call detail records requested on customer initiated telephone calls. If a customer does not elect to establish a password or does not provide a password, the Company will only release call detail information by sending it to an address of record, or by calling the customer at the telephone number of record. For all other CPNI the Company first authenticates the customer before disclosure. The Company has implemented mandatory password protection for online account access that does not use readily available biographical information. Customers are immediately notified via letter to the address of record when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed.

Company personnel are trained as to when they are and are not authorized to use CPNI, and personnel are subject to disciplinary action for failure to comply with CPNI rules. Specifically, upon employment, all personnel must acknowledge they have read and understand the Company's Customer Confidentiality and Communications Policy and sign an agreement. In addition, information relative to CPNI and applicable CPNI rules are posted on the Company's intranet homepage and included in the Company's Voice Customer Service Manual.

The Company keeps records of its sales and marketing campaigns that use CPNI. Specifically, the Company completes a report for each campaign including a description of the campaign and the customers targeted by the campaign. Customers who have elected not to permit the disclosure of their CPNI are excluded from the campaign. The records are maintained for a minimum of one year. If CPNI is provided to third parties, the Company would maintain records of that provision for a minimum of one year. Customers who have elected not to permit the disclosure of their CPNI, via the opt-in process, are excluded from the campaign.

The Company has established a supervisory review process regarding carrier compliance with the CPNI rules. Specifically, the Company has acknowledgements from each of its employees that they have read and understand the Customer Confidentiality and Communications Policy. Second, the Company's Voice Customer Service Manual outlines CPNI rules. Finally, the importance of protecting the confidentiality of CPNI is raised and stressed at each staff meeting and all employees with access to the customer record system are aware that all access to CPNI is monitored and identified internally by the system.

The Company shall notify law enforcement of a breach of its customers' CPNI no later than seven business days after a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).